

REMARKS

Overview

Claims 1-11 remain in the application. No claims have been canceled. No claims have been amended. No new claims have been added.

The rejection of independent claims 1, 6, and 11 under 35 USC 103(a), as being unpatentable over Stewart¹ in view of Cuomo² is hereby respectfully traversed, and reconsideration thereof is requested, in view of the reasons and remarks set forth below.

Claims 1, 6, and 11 Are Patentable Over the Cited References

Claims 1, 6, and 11 all recite, in pertinent part sending an initialization code to a first chaotic system to generate an unpredictable first key bitstream, and sending the same initialization code to a second chaotic system, identical to the first chaotic system, to drive the second chaotic system into synchrony with the first chaotic system and to cause the second chaotic system to generate a second key bitstream, which is identical to the first key bitstream.

As explained in the specification (p. 3, last line and p. 4, lines 1–2), an important advantage of the method of the invention is that the actual key is never transmitted (rather, it is generated remotely at the second chaotic system). As further explained, no information is ever transmitted from which the digital key or the chaotic system could be reconstructed. Notably, as explained on p. 3, lines 7–9 of the instant specification, even if the initialization code, which is transmitted from the first chaotic system to the second chaotic system, is intercepted, it cannot be used to reproduce either the key bitstream or the chaotic system.

¹ U.S. Patent No. 5,592,555.

² *Synchronization of Lorentz-Based Chaotic Circuits with Applications to Communications*, IEEE Transactions on Circuits and Systems, Vol. 40, No. 10, pp. 626–633, October 1993.

Stewart fails to teach or suggest anything relating to employment of chaotic systems for secure communications. Stewart also fails to teach or suggest the use of an initialization code, which contains no information from which an encryption key can be determined, to synchronize two chaotic systems to remotely generate an encryption key, as recited in claims 1, 6, and 11.

In contrast, Stewart, at col. 7, lines 1–21 (referring to Fig. 5) (cited by the Office Action), discloses a method of performing authentication (not key generation) by directing a generated phone identifier 174 and a random number 176 (in base station 12) to a privacy function 178 that performs an enciphering function, thus producing an expected response 186. The random number 176 is sent over the air interface 172 to the handset 14, combining with a second phone identifier 180 (locally generated at the handset) to cause a second privacy function 182 (identical to privacy function 178 of base station 12) to produce an output that is sent back over the air interface 172 to the base station, to be compared, by matching function 184, with expected response 186 in the base station.

Col. 7, lines 62–67 and col. 8, lines 1–18 of Stewart (referring to Fig. 6), also cited by the Office Action, disclose a method of generating a session key 198 and using the key to produce a pseudo-random bitstream 208; the logical XOR circuit 210 combines the pseudo-random bitstream with clear data stream 212 to produce a masked “secure” data stream to be transmitted over the air interface. Lines 35–50 of col. 8 of Stewart (cited by the Office Action) mainly disclose that the pseudo-random bitstream 208 may be duplicated on the other side of the air interface.

The random number 176 of Stewart is functionally distinct from Applicant's recited “initialization code”, and cannot serve as an initialization code for any chaotic system. The same can be said about Stewart's expected response 186 (or 194), because the expected response is the product of the random number applied to the privacy function 178.

More particularly, as explained in the specification at p. 11, last line, and p. 12, lines 1–2, the recited initialization code is a sequence of controls applied to each of the

chaotic systems to drive them into synchrony, by driving them onto identical periodic orbits (see). An initialization code is not a random number generated by a random number generator (in contrast to Stewart's disclosure). In fact, not every bitstream can serve as an initialization code. For example, as the present application states, "certain controls may be used as initialization codes." (p. 5, lines 4–5). Not every sequence of bits from a random number generator would cause a chaotic system to assume a periodic orbit. Additionally, Stewart does not disclose anything to indicate he even contemplated using his random number to synchronize two chaotic systems.

In further contrast to the inventions of claims 1, 6 and 11, where an attacker cannot determine any information about any key due to the recited use of the "initialization code", Stewart explains at col. 7, lines 34–39, an attacker can determine his enciphering key by monitoring the air interface. It is this type of prior art deficiency that the recited use of initialization codes in claims 1, 6 and 11 avoids by not transmitting the key (nor anything from which the key or the dynamics of the chaotic systems can be inferred), and instead recites generating the key at the second chaotic system.

Cuomo fails to remedy the deficiencies of Stewart. In contrast to the recited invention, Cuomo teaches using a "drive signal," but Cuomo's "drive signal" is not equivalent to the recited initialization code. Unlike the recited initialization code, which, as described on p. 3, lines 7–9 of the instant specification, reveals no information about the chaotic systems, Cuomo's "drive signal" is a chaotic signal that reveals information about the state and dynamics of the chaotic systems.

Cuomo employs what is commonly referred to as additive chaos masking. A known drawback of additive chaos masking is that an attacker can infer the dynamics of the first chaotic system, determine the masking signal, and subtract the masking signal from the transmitted information to reveal a masked message signal. As the recited invention employs an "initialization code," not a "drive signal," no such dynamic information may be inferred from information transmitted between the first and second chaotic systems.

Applicant submits herewith a Supplemental Information Disclosure Statement (IDS), which includes a paper titled "A Survey of Chaotic Secure Communication Systems," by Tao Yang. Yang describes the chaotic signal masking approach of Cuomo (see Yang, p. 84, first paragraph of section 2.1, and p. 85, Fig. 1(a)). Yang also discusses the drawbacks of Cuomo's system (see Yang, p. 88, second paragraph). In particular, Yang cites a paper by Kevin M. Short (Applicant), titled "Steps Toward Unmasking Secure Communications" (also included in the IDS submitted herewith). Both of these papers further discuss how, in contrast to the use of initialization codes, recited in claims 1, 6, and 11, subtracting Cuomo's masking signal from the transmitted information reveals the masked message signal.

For at least the reasons that Stewart does not teach or suggest anything relevant to the use of chaotic systems for remote key generations, and that neither Stewart nor Cuomo, nor any combination thereof, teaches or suggests the recited use of an "initialization code," Applicant respectfully requests that the Examiner reconsider and withdraw the rejection of claims 1, 6, and 11. As claims 2-5 and 7-10 variously depend from claims 1, 6, and 11 and recite further limitations thereon, Applicant also respectfully requests that the Examiner reconsider and withdraw the rejection of those claims.

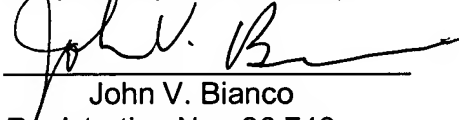
CONCLUSION

In view of the above remarks, Applicant submits that claims 1-11 are in condition for allowance, and requests that the Examiner pass this application to allowance.

If the Examiner believes that a telephone conversation with Applicant's attorney would expedite allowance of this application, the Examiner is invited to call the undersigned.

Dated: 04 February 2004

Respectfully submitted by,



John V. Bianco
Registration No.: 36,748
ROPES & GRAY LLP
One International Place
Boston, Massachusetts 02110-2624
(617) 951-7000
(617) 951-7050 (Fax)
Attorney/Agent for Applicant

NOTE: It is believed that fees due in connection with this submission have been appropriately provided. However, if an additional fee amount is due, please charge Deposit Account No. 18-1945, under Order No. CAOT-P02-001, from which the undersigned is authorized to withdraw.